	GEORGIA TECHNOLOGY AUTHORITY	
Doc Ref Number:	ENT-09-001-STD	**Topical Area: Telecommunications and Network**
Document Type:	Enterprise Standard	**Page:** 1 of 24
Title:	**WLAN (WiFi) Standard**	
Effective Date:	2/1/2006	
POC for Changes:	Georgia Wireless Standard Committee (GWSC)	
Synopsis:	To establish standards that encourage wise decisions when engaging in the usage of WLAN (WiFi) technologies.	

TABLE OF CONTENTS

Stakeholders

Name	Stake in Project	Organization	Title
Patrick Moore	Executive Sponsor	Office of the Governor (GOV)	Deputy Chief Operating Officer
Tom Wade	Business Owner	GTA	Chief Executive Officer
Charlie Sasser	Executive Sponsor of Work Group and Wireless Trials	GTA	Director of Support Services
Kimberly Gordon	Subject Matter Expert	GTA	Enterprise Architect
Wireless Oversight Committee	**Executive Committee –** State of Georgia Agencies		Executives from Various Agencies
	Hanna Hecke, GOV Tom Maier, BOR Randall Thursby, BOR Jim Flowers, BOR Mike Hall, DOE John Stewart, DHR Dee Ford, DEcD	Frank Howard, DTAE Mike Nixon, GPB Tony Mazza, P&P Cigdem Delano, GTA Renee Herr, GTA Steve Nichols, GTA Suhas Uppalapati, GTA Robert Woodruff, GTA	
ISO Council	Defining and verifying security requirements	State of Georgia Agencies	All Information Security Officers (ISO)
CIO Council	Final approval for operational turnover and Implementation	State of Georgia Agencies	All Chief Information Officers (CIO)
Wireless Standards Work Group	**Team Members –** State of Georgia Agencies		Wireless Experts
	Bruce Bailey, DHR Rory McClure, DHR Walter Tong, DOE Geoff Catron, DTAE Steve Ferguson, DTAE Matt Sanders, GaTech Dan Brown, GEMA Chip Eberhart, GPB Mike Nixon, GPB	Eric Harris, GSP Brent Williams, KSU[i] Bob Grafals, GTA Chuck Jordan, GTA Denise Techmeier, GTA, Program Technical Writer Jim Mollohan, GTA, Program Business Owner Wray Hall, GTA	

[i] Kennesaw State University

PURPOSE

To define the 802.11[ii] standards for agencies to use in deployment of wireless technology.

INDUSTRY STANDARD

This policy applies to the use of wireless technologies deployed on an agencies' wireless local area network (WLAN). The dominant standards to date have been the 802 standards series developed by the Institute of Electrical and Electronic Engineers[iii] (IEEE). Any use of wireless strategy should comply with the most current version of the IEEE 802.11 standard. The current version of 802.11 can be found at http://grouper.ieee.org/groups/802/11/. To further standardize the use and deployment of 802.11 in the State of Georgia's environment, the following areas are clarified in this policy adoption: security, rogue and foreign access points, signal coverage and access point placement, network management, certification / interoperability, service levels, power over Ethernet (PoE), quality of service (QoS), guest access, roaming, deployments and systems.

Although many government entities have already started using wireless technology, the intent of this document is to outline areas that need to be reviewed and explain areas that need to be considered on initial deployment.

The following standards are in commercial, office and industrial use: IEEE's 802.11a, 802.11b, 802.11g and 802.11i. These standards will serve as the de facto WLAN standards for the State. Whenever deploying a WLAN solution, agencies must insure vendors meet these standards. A summary of the standards and a comparative table are below. This document will be updated as applicable standards are ratified by IEEE.

[ii] *802.11* refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

[iii] IEEE, pronounced I-triple-E, was founded in 1884 as the AIEE. The IEEE was formed in 1963 when AIEE merged with IRE. IEEE is an organization composed of engineers, scientists and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.

IEEE 802 Standard	Description	Definition
802.11a	- Mandates support for data rates of 6, 12, and 24 Mbps - Works only in 5 GHz Unlicensed National Information Infrastructure (UNII)[iv] Bands	802.11a is a faster version of 80211.b, which supports speeds up to 54 Mbps and runs in the 5 MHz range. Specifically, speeds of 5.15 MHz to 5.35Mhz for indoor use and 5.725 MHz to 5.825 MHz for outdoor use. The FCC allocated the range in support of UNNI. The 802.11a standard is also called WiFi 5, for the Wireless Fidelity in the 5 MHz range. This standard divides the spectrum into 52 channels, 48 of which are for data transmission. The other four are for error control….depending on how fast the modulation is for each channel, and how many channels are available.

[iv] The 5 GHz bands are made up of three separate 100 MHz-wide bands which are used by 802.11a compliant devices. The FCC restrictions on these bands include for UNII-1 (5.15 GHz to 5.25 GHz) has the maximum output power of 40mW and the devices used in the band are restricted to indoor use. UNII-2 (5.25 GHz to 5.35 GHz) is specified at 200mW of output power and devices can be used indoors or outdoors. UNII-3 (5.725 GHz and 5.825 GHz) is specified to 800 mW and devices are outdoor, long-distance links.

IEEE 802 Standard	Description	Definition
802.11b	- Specifies Direct Sequence Spread Spectrum (DSSS) technology - Mandates support for data rates of 1, 2, 5.5 and 11 Mbps - Works only in 2.4 GHz Industrial, Scientific, Medical (ISM)[v] Bands	This is the most common standard for wireless LANs. It is used in offices, airports, hotels, coffee shops, homes, and offices around the world. The 802.11b standard operates in the unlicensed 2.4 GHz range (2.4 to 2.483 GHz). Many other devices operate in this range (such as microwaves, garage doors, barcode scanners, cordless phones), and can negatively impact performance. 802.11b is also known as WiFi. This standard provides for speeds up to 11 Mps and distances of 1600 feet. 802.11b provides for low power wireless systems, which mean the closer to the transmitter the faster the speed, and the further from the transmitter the slower the speed. The 802.11b standard divides the spectrum into 14 channels. However in the US, the FCC allows the use of 11 channels. Adjacent channels overlap and interfere with each other, so deploying multiple access points requires careful planning.

[v] ISM is an acronym for Industrial, Scientific and Medical. This refers to the unlicensed radio bands which are typically unused due to interference from medical, industrial and scientific equipment. Technologies such as Bluetooth and Wireless LANs use these bands since no governmental approval is needed for transmission, making it a great deal cheaper. Whilst interference is still an issue, technologies for overcoming it are built into most technologies using these bands.

IEEE 802 Standard	Description	Definition
802.11g	- Specifies Orthogonal Frequency Division Multiplexing (OFDM) and DSSS technology - Mandates support for data rates of 6, 12, and 24 Mbps OFDM - Supports 6, 9, 12, 18, 24, 36, 48, 54 Mbps OFDM - Works only in 2.4 GHz ISM Band	The 802.11g standard provides for speeds up to 54 Mbps in the 2.4 GHz range. Devices that use 802.11b and 802.11a are not compatible with each other, but 802.11g devices work with both standards.

IEEE 802 Standard	Description	Definition
802.11i	- Specific to wireless LAN security - Specifies 802.1x / EAP, AES and other technologies introduced to enhance security beyond 802.11 - WPA v1.0 is a stop-gap standard from the WiFi Alliance - WPA v2.0 will be fully 802.11i compliant	The 802.11i specification addresses key weaknesses in the 802.11 security model that were first exposed in 2001 when researchers discovered fundamental flaws in the 802.11 Wired Equivalent Privacy (WEP) encryption mechanism. By adding support for the more robust Advanced Encryption Standard (AES), 802.11i offers much stronger privacy services. 802.11i also includes a well defined authentication mechanism based on the existing 802.1X and Extensible Authentication Protocol (EAP) framework. By combining AES and 1X/EAP, dynamic key management tied to user authentication is now available on 802.11 networks through a standardized protocol suite. Previous attempts to implement authentication with dynamic keys were largely proprietary. Not only does 802.11i provide for authentication and privacy, it also paves the way for role-based authorization services on wireless LANs, where network access permissions are tied to user credentials and group membership. The 802.11i standard replaces the Rivest Cipher 4 (RC4) encryption engine used by WEP and WPA with Advanced Encryption Standard (AES) encryption. The WiFi Alliance has created WiFi Protected Access version 2 (WPA2) as a certification suite for 802.11i products. The full 802.11i standard supports preauthentication and roaming. In addition to transferring encryption keys between APs, preauthentication reduces transfer time between APs from 600 milliseconds to 30 milliseconds or less. For enterprises running VoIP on their WLANs, this important feature will keep voice calls from being dropped.

Capability Comparison

	802.11a	802.11b	802.11g
Maximum data rate	54 Mbps	11 Mbps	54 Mbps
Operating frequency	5 GHz	2.4 GHz	2.4 GHz
Range	300 ft/100 m	300 ft/100 m	300 ft/100 m
Non-overlapping channels	24	3	3
Interference sources	Cordless phones, radar, satellite (Europe only)	Bluetooth, microwave ovens, baby monitors, video cameras, lighting systems	Bluetooth, microwave ovens, baby monitors, video cameras, lighting systems
Standard approved	Yes	Yes	Yes
WiFi certified	Yes	Yes	Yes
802.11b compatible	No	N/A	Yes

A significant challenge in providing wireless access is the protection of the computer networks connecting the wireless devices. These challenges include ensuring that:

- Only authorized users are allowed access to the network;
- Confidential information is secure during data transmission; and,
- The network is available and protected against malicious attacks.

STANDARD FOR THE STATE OF GEORGIA

In order to address the risks associated with wireless computer networks, the State of Georgia has established a wireless network access policy (Policy 9.4.2). The policy requires agencies to take "appropriate steps, including the implementation of strongest-available encryption, user authentication, and virus protection measures, to mitigate risks to the security of State of Georgia data and information systems . . . ." the State of Georgia's standards require agencies to develop a wireless LAN Implementation Procedure Plan, assess the risks posed by a wireless network, mitigate those risks, and conduct periodic reviews to ensure that the network is secure. The standards prohibit open unsecured wireless network access technology.

The ISO Council has adopted the National Institute of Standards and Technology (NIST) 800 series as the security guidelines. Wireless security is specifically addressed in the following NIST standards:

- NIST 800-18 Guide for Developing Security Plans for IT Systems
- NIST 800-46 Security for Telecommuting and Broadband Communications
- NIST 800-48 Wireless Network Security: 802.11, Bluetooth and Handheld Devices

Use 802.3f, specification of Power over Ethernet (PoE), to enhance AP operation via a stable power source and to simplify installation process throughout the enterprise.

Wireless Local Area Networks (WLANs) should at the minimum implement WPA (WiFi Protected Access) for security, but full 802.11i compliance is a standard with components and equipment that can adhere to 802.11i.

For areas not mentioned in this section, seek guidance in the external sources mentioned in the "Standards" section.

Understanding the limitations and capabilities of the wireless technologies, the following areas will be considered in the establishment of WiFi policies:

- Use 802.11g where:
  - Higher-speed WLANs operating in the 54 Mbps to will provide improved throughput for applications requiring greater speed (IEEE 802.11g)
  - Improve throughput and maintain backward compatibility with 802.11b by using 802.11g[vi] in areas covered by 2.4 GHz band.
- Use 802.11i (security) to protect connection to networks, reduce and / or eliminate signal leaks outside the enterprise through building walls, floors, and ceilings by defining the:
  - access to the wireless network based on physical proximity
  - management of individual ports to wired networks

[vi] IEEE 802.11g allows for data rates up to 54 Mbps by using orthogonal frequency-division modulation (OFDM), the same modulation technique used in the 802.11a standard. IEEE 802.11g achieves backward compatibility with 802.11b by using the same methods of modulation for data rates less than or equal to 11 Mbps.

    - protection mechanism of transmitted data to prevent interception and decryption
- Use wireless network management tools to control signal levels, coverage areas, interference sources and other WLANs
- Adherence to newly IEEE certified products to ensure cross product compatibility
- Use testing mechanism to certify devices
- Define and document Quality of Service (QoS) requirements when voice and video are used on the WLAN
- Define and document guest access policies
- Use and creation of IP tunnel from a home antenna to a different antenna with the same IP address and authentication credentials
- New network interface cards (NICs) for mobile equipment should support 802.11g for full compatibility with both the enterprise networks and external hotspots.
- MAC address should not be the total security solution because MAC address resolution alone does not qualify as strong authentication.

Security

There should not be any unnecessary services/applications running on the machines connected to the WLAN. Wireless communications shall be disabled upon PC being docked into a wired LAN via the hardware profile. Strongest available standards-based commercially available encryption should be employed with maximum key length and should be upgraded as newer technology is available. WEP should not be used.

- The Service Set Identifier (SSID) shall in no way identify with the owner of the network and default SSID's shall not be used.
- Lockdown procedures shall be performed on wireless enabled laptops to protect against unauthorized accessing of shared drives, services, etc. Lockdown is defined as the limiting of user capability to reconfigure the laptop/pc by allowing certain options to only be changed by an administrator.

Authentication

All currently implemented State wireless solutions must fully meet strong identification and authentication requirements. These requirements should be an extension to a LAN environment.

Strongest Authentication Possible

Authentication Technique	Strength	Weakness
LEAP	Simple, ubiquitous	Cisco proprietary, known vulnerabilities
EAP FAST	Simple	Limited support
PEAP	Future path, wide auth server support	Complex, immature, interoperability issues
EAP-TLS	Interoperability	Complexity

VPN	Easy, rapid start up	User resistance, potential complexity

Agencies should not make any major investments in a new WLAN technology if it does not support WPA2 and multiple authentication types. Agencies that have WLAN systems deployed today using WEP, should upgrade to a vendor product that support temporal key integrity protocol (TKIP) for frequent key changing.

As soon as the technology is available, agencies should use WPAS and a standard version of PEAP to secure their networks.

The public key infrastructure (PKI) and digital certificates will be used to the greatest extent possible to support security solutions. Security solutions using digital certificates must comply with the State of Georgia's PKI requirements. When external certificate authorities are necessary, issuance of certificates plans for key escrow, and revocation of user certificates will be documented.

Encryption

WLAN security requires several different components. Encryption prevents the data from being intercepted and decoded when it is broadcast over the WLAN; authentication allows only authorized users access to the WLAN.

Because WLAN signals may extend outside the network's physical premises, it is possible for an interloper to gain access to a LAN using an IEEE 802.11-equipped portable computer outside of the building or in an adjacent office, whether that office is above, below, or next to the enterprise office. The solution to such interception is to encrypt the information broadcast on the RF link. The encryption alternatives include:

- WEP, an extension to IEEE 802.11, provides very limited security for data transmissions by scrambling the data before it is transmitted over radio waves. WEP was intended to prevent interception of WLAN signals, but use of static keys, lack of automated key management, weaknesses in the key scheduling algorithm, and improper implementations of the cryptographic engine leave WEP-protected WLANs open to interception by attackers with minimal equipment and effort. WEP should be used only as a first line of defense, or at a minimum, as a "Keep Out" sign that identifies a private network. As inadequate as WEP is, it is better than no security at all, and when coupled with 802.1x authentication mechanisms that provide different keys for each associated station, WEP can offer security from inadvertent intruders. Again, agencies that have WLAN systems deployed today using WEP, should upgrade to a product that supports TKIP for frequent key changing.
- The WiFi Alliance's WPA version 1 solution was a snapshot of the 802.11i security committee's early work. WPA implemented the parts of the 802.11i standard that were stable, thus allowing a much higher level of security than WEP. The functionality of WPA includes: Authentication and key generation using 802.1x mechanisms, Basic service set (BSS) infrastructure mode operation, A key

hierarchy that is derived from a session key, Automated key management services, Cipher and authentication negotiation services, Temporal Key Integrity Protocol (TKIP) and Improved Message Integrity Check (MIC[vii]).

Secure Network - VPN

VPNs offer both authentication and encryption. Whether Internet Protocol security (IPsec)- or Secure Sockets Layer (SSL)-based, VPNs can be used to encrypt the data transmitted between a station and an AP. This ensures that even if the data is intercepted. This is especially critical when stations are connected to nonencrypted APs such as those found in most public hotspots. Some WLAN systems include VPN capabilities in their controllers. For most environments, separate VPN controllers will be needed to provide the same capabilities for all users of the VPN regardless of their connection method.

VPNs are not required for security when mobile users are connected to an 802.11i-secured WLAN. However, use of VPNs on mobile devices is needed when users are accessing the network through unsecured connections.

- Create a wireless DMZ and have users authenticate through the VPN
- Use RADIUS[viii] authentication

[vii] MIC prevents bit-flip attacks. It should be implemented on both the access point and all associated client devices. MIC adds a few bytes to each packet to make the packets tamper-proof.

[viii] **RADIUS** (**Remote Authentication Dial In User Service**) is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

When you connect to an ISP using a modem, DSL, cable or wireless connection, you must enter your username and password. This information is passed to a Network Access Server (NAS) device over the Point-to-Point Protocol (PPP), then to a RADIUS server over the RADIUS protocol. The RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP. If accepted, the server will then authorize access to the ISP system and select an IP address, L2TP parameters, etc.

The RADIUS server will also be notified when the session starts and stops, so that the user can be billed accordingly; or the data can be used for statistical purposes.

RADIUS was originally developed by Livingston Enterprises for their PortMaster series of Network Access Servers, but later (1997) published as RFC 2058 and RFC 2059 (current versions are RFC 2865 and RFC 2866). Now, several commercial and open-source RADIUS servers exist. Features can vary, but most can look up the users in text files, LDAP servers, various databases, etc. Accounting tickets can be written to text files, various databases, forwarded to external servers, etc. SNMP is often used for remote monitoring. RADIUS proxy servers are used for centralized administration and can rewrite RADIUS packets on the fly (for security reasons, or to convert between vendor dialects).

RADIUS is extensible; most vendors of RADIUS hardware and software implement their own dialects.

The DIAMETER protocol is the planned replacement for RADIUS, but is still backwards compatible.

1.1 DEVICES

Devices should be compatible with access points, 802.11 and the security strategy outlined by the MAC, authentication, encryption strategies chosen by GTA and the engaging Agency. Handheld Devices will be addressed in a separate document relative to procurement needs.

Prior to installation of devices where wireless LANs are to be implemented, thorough analysis, testing, and risk assessment must be done to determine the risk of information intercept/monitoring and network intrusion prior to installation of these devices. It should be noted that only properly trained personnel can successfully determine these risk factors.

In deployment

- Use a seamless RF umbrella that delivers the required service level to each mobile device regardless of location
- Use dynamic address assigned to mobile devices for roaming capabilities with encrypted connections
- When implementing a wireless architecture, use encryption to secure user login information when they connect to the LAN. While confidential information must be secured - all formats - (e.g., paper files, electronic documents) or the method in which it is stored and shared (e.g., computers attached to a wired network), personal wireless devices pose specific security concerns. These include the security of data/voice while in transit and the security of data once it is stored in a device and are described as follows:

    - Security of Transmissions – The use of radio waves for the transmission of data / voice makes the interception of the information by a third party possible. In addition, personal wireless devices allow employees to conduct business in public places, where confidential information discussed in a cell phone Deconversation may be overheard or confidential information entered into a PDA may be seen by a bystander.
    - Security of Stored Information – Personal wireless devices are generally small, mobile devices that can be easily lost or stolen. Devices may have confidential files, emails, or other forms of information that would be accessible if the device does not employ adequate security measures.

In order to address these security concerns, agencies mustadopt a policy stating whether confidential information will be permitted to be transmitted to/from personal wireless devices or stored on those devices. If confidential information is to be allowed, agencies' policies should consider the following:

- Procurement of wireless devices and services must include consideration of the security features of the device. Procurement is frequently based on just the availability of wireless service in a geographic area and the price.

- Agency end user training should train individuals should always be aware of their surroundings when using personal wireless devices. For example, confidential information should not be discussed on a cell phone if the user is in a public area. Likewise, individuals should be careful when viewing documents and files containing confidential information on their wireless PDA or Blackberry device.
- Agencies should have policies addressing the steps to be taken if a personal wireless device is lost or stolen. The individual assigned the device should immediately report the missing device to an appropriate agency contact that should have the service disconnected.
- Personal wireless devices should require individuals to enter a password before using the device. This is most applicable to devices such as Blackberry devices and wireless PDAs that may contain stored files or documents with confidential information.

Various wireless, wired interconnection capabilities and multi-capable functioning of devices present a significant risk handling classified or sensitive information transported over unclassified mediums. All devices should have strong identification and authentication (I & A)[ix] used to store, process, or transmit official GTA or Agency information. Devices without strong I & A built in or added to the system will only be used for administrative tasks, such as maintaining appointment calendars and non-sensitive contact lists.

Web-enabled devices that rely on wireless access protocol (WAP) and or use commercial wireless network providers are at risk for information compromise. Data will not be transmitted in this situation unless the data is encrypted end-to-end using a FIPS-validated crypto module. When WAP gateways are installed in the top-level architecture (TLA) of State networks to provide access to web-servers, they will be properly controlled and monitored by firewalls and intrusion detection systems (IDS).

State employees using devices that synchronize with desktop or laptop computers on the GTA networks will adopt the following security measures:

- Use applications that are approved by GTA or the employee's Agency
- Passwords, combinations, personal identification numbers (PIN) and classified information will not be stored on Devices.

1.2 ACCESS POINTS

In the use of access points:

[ix] login and password/pin

- Monitor access via foreign access points (APs) and detection of rogue APs.
- Maximize the coverage and standardize AP placement.
- Use enterprise-class APs that support multiple simultaneous radio technologies (802.11a/b/g/h devices)
- Within the State of Georgia, access points that support 802.11g should be deployed. Since 802.11g provides backward compatibility with 802.11b, using devices that 802.11g will give the capability of connecting with stations using either standard.
- Access points…..These are the configuration guidelines in order of preference:
    - Authentication shall be set to Shared Key Authentication rather than the default Open Systems Authentication to require potential clients to authenticate themselves to the network before allowing connection.
    - WPA/PSK – While using WPA/PSK for authentication and WPA/TKIP for encryption provides a potentially stronger form of security than WEP It is recommended that any group of 10 or more users move to a 802.1x/RADIUS solution for secure wireless access.
    - User Authentication tool (such as ID/password via a RADIUS server) should be employed to increase confidence in authentication of client. This is the ideal method of securing wireless networks. Any 802.11x/RADIUS wireless security solution for small to medium workgroups should be:
        - easy and inexpensive to implement and,
        - provide a simple ongoing management interface that empowers non-technical workgroup users to self-manage the ongoing authentication and de-authentication of wireless clients.
            - All access points shall be established toward the center of the building rather than near the windows. This allows coverage to radiate out to the windows, but not far beyond.
- AP operating system shall be hardened so as to protect the privacy of encryption keys.

1.3 RISK MITIGATION

In mitigating the risks associated with wireless computer networks, all state agencies should:

- Have an IT security policy that addresses wireless computer network related issues. A thorough, well-enforced policy can protect an agency from unauthorized access as well as unnecessary performance degradation. Policies for all state agencies should forbid unauthorized access points and ad-hoc networks that can circumvent network security.

- Search for rogue wireless computer networks. Since wireless computer network packages can cost less than $200 and are easy to install, employees may be tempted to deploy unauthorized wireless computer networks. These rogue wireless computer networks may have standard security features turned off and have the potential to circumvent an agency's network security. Procedures to search for rogue wireless computer networks include performing physical inventories and conducting periodic scans. In mitigating the risks associated with wireless computer networks, state agencies using wireless networks should:
    - Continually monitor the network. A wireless computer network should be monitored for a variety of activities such as: rogue wireless access points logging on and off the system; and overall use of the network.
    - Change the Service Set Identifier (SSID). The SSID is an identification string that enables clients to initiate connections. If the default (manufacturer's setting) is used or if an SSID that might call a potential hacker's attention to valuable information is used, this may increase the risk of attacks. GTA policy 9.4.2 states that "the Service Set Identifier (SSID) shall in no way identify with the owner of the network and default SSIDs shall not be used."
    - Agencies using Wired Equivalent Privacy (WEP) must upgrade their systems with additional protective measures or to the new 802.11i(WPA2) standard. WEP is a standard security feature found on most wireless computer networks that helps to prevent casual "eavesdropping" by unauthorized parties. However, WEP lacks a strong encryption algorithm. By gathering the data transmitted, an attacker can break the encryption code. WEP has been broken in less than 15 minutes. Since WEP's encryption method provides inadequate protection against intruders, agencies must upgrade to (Temporal Key Integrity Protocol)TKIP or the new 802.11i(WPA2) security standard.

1.4 NEXT STEPS

The authentication decision should happen within the following timeline.

Now

- Extend existing secure WLAN with TKIP, monitoring
- Choose vendor solution(Cisco PEAP/EAP FAST, MSFT PEAP, Funk)
- Plan refresh, migration by 1Q07

3Q06

- Choose WPAx, converged PEAP approach
- Focus on integration to wired side authentication/access control

1.5 AUDITING

The areas that will be reviewed during a best practices audit include:

- Was the system deployed using user based authentication? This will secure the wireless connection, allow easy revoking of privileges, offer usage of static devices and achieve usage of 802.1x or VPN.
- Was a bluesocket, SSL or IPsec VPN approach used? This will encourage VPN termination close to the AP, supports 802.1z, and enables hybrid deployment of APs.
- Is the site survey information available? Were directional antennas used? This will minimize the amount of RF spilling.
- Are the wireless LANs on their own VLAN? This minimizes the risk of layer attacks.
- Are there any backdoors in the system? Check with a wireless sniffer, directional antenna and WiFi card with (internal channel hopping, external antenna connection, etc.). Do a “black box[x]” and “white box[xi]” testing. This will keep intruders from impersonation.
- Does the deployment of 802.1x allow secure from / for unauthorized access, authorized access, administration access, strong passwords, lock-out, login/logout logging? This secures the LAN.
- Are anti-virus, personal firewalls certificates and mutual authentication in use?
- Is dynamic key exchange being used?
- Who can reset APs and are the APs physically secure? Do APs have strong passwords?
- Are static IP addresses being used?
- In general has proper security configuration been used to allow network administrators to find vulnerabilities and / or capture wireless packets? Does the system:
    - Track beacon packets to find all access points
    - Determine SSID and AP name
    - Track probe packets and probe responses
    - Track data packets
    - Determine link encryption packets, firmware versions and authentication packets.
        -
- Is the system using secure protocols? Are EAP, TKIP and MIC or the equivalents in use?

1.6 EXCEPTIONS

GTA must approve all exemptions to this standard.

[x] Black Box testing includes coverage map, physical security of AP, SSID review, use of encryption, channel separation, unpredictable user names / passwords and denial of service.

[xi] White box testing includes use or avoidance of VLANs, no servers on wireless VLAN, redundancy, what is on the wire once logged in, automatic access to wireless and broadcast key rotation.

BEST PRACTICES

To avoid trap doors that occasionally open during the deployment of enterprise WLANs, it is vital that IT project managers and network designers follow best practices that address everything from the placement of access points, to the adjustment of antennas.

Best Practice #1: Leverage Existing Network Infrastructure

Most companies already have an architecturally consistent wired network infrastructure in their campus buildings. Overlay the existing wired network with a wireless subnet, leveraging the strengths of both. On this subnet, attach access points, which are wireless bridges that allow mobile clients to communicate with wired Ethernet infrastructures."

Best Practice #2: Perform a Professional Site Survey

The site survey is a hands-on assessment of the number of access points and antennas need, and where to place them. Using specialized site survey tools, surveyors walk the entire building that is to be wired, testing signal strength from various locations. Through this "can you hear me now"-like process, they identify the best locations for access points. The thoroughness of this survey will help achieve proper radio frequency coverage throughout the enterprise.

Best Practice # 3: Design for Multi-Site Consistency

A major goal in any campus-wide WLAN deployment is to achieve—to the degree possible—multi-site consistency in network architecture and equipment. In buildings that are laid out the same way, a single network design will probably work throughout. However—and this is very important—if this company's campus has buildings of different shapes and sizes, then each WLAN subnet will have to be customized to accommodate the unique characteristics of the building in which it is deployed.

Architectures may differ, but the network hardware should not. Network equipment, even when expanding an existing network into a building that may be newly acquired and unwired, should be consistent with that in other buildings.

Best Practice # 4: Design WLAN for Optimal Roaming

The entire purpose of a wireless network is to support mobility. In a multi-building network, however, the ability to roam without signal interruption can become difficult as mobile workers cross from one wireless subnet to the next. This problem can be exacerbated by some security solutions that restrict users to a single subnet.

WiFi standards 802.11b and 802.11g feature three non-overlapping channels that should allow network designers to easily avoid overlap.

Best Practice # 5: Implementing Wireless LANs

Wireless solutions must be able to detect and suppress rogue access points. Design access controls that only allow authorized devices and users access to the wireless network.

Wireless solutions must incorporate a location aware protection scheme. This means the security policies are enforced based on location, the connection interface (for example, a PCMCIA card), and the wireless access points. *This measure is for both home and traveling.*

The security approach should be a multilayer approach. Where devices have firewalls, use them within the wireless strategy as dictated by wireless architecture when high security is needed.

Wireless solutions will create backdoors into GTA LANs if not implemented properly. If a device receives information via a wireless technology, and that device allows that information to be placed directly into the LAN at the workstation level, then all perimeter and host-based security devices have been bypassed.

Best Practice # 6: Consider security threats to mobilized workers whenever making deployment decisions

Minimize the opportunities for hacking, theft, unauthorized access (spoofers), electronic eavesdropping (sniffers) and tampering of data by continuously increasing security mechanisms.

Best Practice # 7: Use of 802.11b

If it is necessary to use 802.11b to APs, performance of all users of that AP will slow up network services for all.

TERMINOLOGY

DSSS

Direct Sequence Spread Spectrum is one of two types of spread spectrum radio, the other being frequency-hopping spread spectrum. DSSS is a transmission technology used in local area wireless network transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

Hotspots

Wireless LAN (local area network) that provides Internet connection and virtual private network (VPN) access from a given location. For example, a business traveler with a laptop equipped for WiFi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.

iDEN

iDEN (Integrated Digital Enhanced Network) is a mobile communications technology that provides its users with the benefits of a trunked radio and a cellular telephone. iDEN places more users in a given spectral space, as compared to analog cellular systems, by using Time Division Multiple Access (TDMA). Six communication channels share a 25 kHz space. Some competing technologies place only one channel in 12.5 kHz. Data (such as paging, text messaging and voice communications) are supported by iDEN. iDEN is a technology with no clear path for high speed wireless data.

Interface

A protocol of behavior that can be implemented by any class, anywhere in the class hierarchy. An interface defines a set of methods, but does not implement them. A class that implements the interface agrees to implement all the methods defined in the interface, thereby agreeing to certain behavior.

MAC

The Media Access Control address is a unique numeric identifier that is programmed into a wireless network interface card by the manufacturer. Some manufacturers allow this identifier to be reprogrammed by the user, therefore it must be assumed that the MAC address can be copied electronically (spoofed).

Mobile

Specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems. These systems operate in licensed bands below 3.5 GHz, optimized for IP-data transport, with peak data rates per user in excess of 1 Mbps. This specification supports various vehicular mobility classes up to 250 Km/h in a MAN environment and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than those achieved by existing mobile systems.

OFDM

***O**rthogonal **F**requency **D**ivision **M**ultiplexing*, an FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a WLAN, 802.16 and WiMAX technologies use OFDM.

RADIUS

RADIUS (**Remote Authentication Dial In User Service**) is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

- When you connect to an ISP using a modem, DSL, cable or wireless connection, you must enter the username and password. This information is passed to a Network Access Server (NAS) device over the Point-to-Point Protocol (PPP), then to a RADIUS server over the RADIUS protocol. The RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP. If accepted, the server will then authorize access to the ISP system and select an IP address, L2TP parameters, etc.
- The RADIUS server will also be notified when the session starts and stops, so that the user can be billed accordingly; or the data can be used for statistical purposes.
- RADIUS was originally developed by Livingston Enterprises for their PortMaster series of Network Access Servers, but later (1997) published as RFC 2058 and RFC 2059 (current versions are RFC 2865 and RFC 2866). Now, several commercial and open-source RADIUS servers exist. Features can vary, but most can look up the users in text files, LDAP servers, various databases, etc. Accounting tickets can be written to text files, various databases, forwarded to external servers, etc. SNMP is often used for remote monitoring. RADIUS proxy servers are used for centralized administration and can rewrite RADIUS packets on the fly (for security reasons, or to convert between vendor dialects).
- RADIUS is extensible; most vendors of RADIUS hardware and software implement their own dialects.
- The DIAMETER protocol is the planned replacement for RADIUS, but is still backwards compatible.

WEP

Wired Equivalent Privacy, (WEP) a security protocol based on RC4 encryption algorithm, is built into the IEEE 802.11standards for wireless LANs. This standard does not use a FIPS-validated crypto module, and has been found by the cryptographic community to have fundamental flaws. WiFi Protected Access (WPA) version 1, WPA2 (WPA version 2) is a newer security protocol built into the 802.11i standard. It offers better protection using temporal key integrity protocol (TKIP). This protocol was added, so that keys are rotated and encryption is strengthened, but it is still based on the RC4 encryption algorithm. WPA2 version 2 of WPA will use strong AES encryption based on Rijndael algorithm (128, 192 or 256 bit key sizes). WPA2 also adds two strong authentication features: wireless robust authentication protocol or (WRAP), counter with cipher block chaining message authentication code protocol or (CCMP).

WiDen

A software upgrade developed for iDEN enhanced specialized mobile radio (or ESMR) wireless telephony protocol. WiDEN allows compatible subscriber units to communicate across four 25 kHz channels combined for up to 100 kbit/s of bandwidth. The protocol is generally considered a 2.5G wireless cellular technology.

WiFi

Wireless Fidelity is another name for wireless devices running under the 802.11b standard, which operates in the 2.4 GHz range. The name is governed (or marketed) by the Wireless Ethernet Compatibility Alliance (WECA).

WiFi5, or WiFi 5, is a newer version for devices running under the faster 802.11a standard. It operates in the 5 MHz range. Specifically, 5.15 MHz to 5.35Mhz for indoor use, and 5.725 MHz to 5.825 MHz for outdoor use.

WiFi-x is a generic name for devices that support 802.11b and 802.11a.

WMAN

Wireless Metropolitan Area Networks (MANs) are large computer networks usually spanning a campus or a city. They typically use optical fiber connections to link their sites. For instance, a university or college may have a MAN that joins together many of their local area networks (LANs) situated around a site that is a fraction of a square kilometer. Then from their MAN, they could have several Wide Area Network (WAN) links to other universities or the Internet. Some technologies used for this purpose are ATM, FDDI and SMDS. These older technologies are in the process of being displaced by Gigabit Ethernet-based MANs in most areas. MAN links between LANs have been built without cables using either microwave, radio, or infra-red free-space optical communication links.

WiMAX

WiMAX is another name for a set of broadband wireless communication standards, developed under IEEE 802.16, for metropolitan area networks. Originally called WirelessMANT, the name is governed (or marketed) by the WiMAX Forum. This forum was founded by a coalition of wireless companies including Intel, Proxim, and Nokia. (Nokia has now left.) WiMAX was ratified as a standard under the 802.16-2004 specification.

WiMAX is expected to compliment WiFi standards. It provides a wireless alternative to last mile local loops, such as T-1 links. WiMAX should also provide competition for broadband DSL and cable services.

Wireless

Term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part, or all, of the communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

WLAN

A Wireless Local Area Network (Wireless LAN) is a computer network that allows a user to connect without a network cable. A laptop or PDA equipped with a wireless LAN card allows a user move around a building with their computer and stay connected to their network without needing to “plug in” with a cable. The most popular wireless LAN today is called an 802.11b network. Wireless LANs require an access point where all the wireless devices connect. This connection point connects the users to the wired network. The coverage of a wireless access point can span up to 100 m (330 feet) indoors.

Other names for wireless LANs are 802.11, or WiFi. There are also different versions of wireless LANs: 802.11b transfers data at speeds of up to 11 Mbps in the 2.4 GHz radio band. The next version, 802.11a, is supposed to transfer data at speeds up to 54 Mbps in the 5 GHz band. Wireless LANs are a successful and popular widespread technology that is being incorporated into many new laptops as standard equipment.

WPA

WPA (WiFi Protected Access) is an interim standard by the WiFi Alliance. WiFi Protected Access is a specification of security enhancements that increases the level of data protection and access control for existing WiFi networks.

WPA will most likely be rolled into the eventual IEEE 802.11i standard.

WPA2

IEEE 802.11i (also known as WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks (see WiFi). The draft standard was ratified on 24 June, 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. WiFi Protected Access (WPA) had previously been introduced by the WiFi Alliance as an intermediate solution to WEP insecurities. It implemented a subset of 802.11i

WPAN

Wireless Personal Area Network (WPAN) is a personal area network that is used for interconnecting devices centered on an individual person's workspace where the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about a very short range, such as 10 meters. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

A WPAN can interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today. It can also serve a more specialized purpose such as allowing a surgeon and other team members to communicate during an operation.

A key concept in WPAN technology is *plugging in*. In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other), or within a few kilometers of a central server, they can communicate as if they are connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug in to any other device in the same WPAN, provided they are within physical range of one another. In addition, WPANs worldwide will be interconnected.

WWAN

A Wireless Wide Area Network (Wireless WAN), covers a much more extensive area than wireless LANs. Coverage is generally offered on a nationwide level with wireless network infrastructure provided by a wireless service carrier (for a monthly usage fee, similar to a cellular phone subscription). While wireless LANs are used to allow network users to be mobile within a small fixed area, wireless WANs are used to give Internet connectivity over a much broader coverage area. For instance to meet the requirements of users such as business travelers or field service technicians. Wireless WANs allow users to have access to the Internet, e-mail, and corporate applications and information while away from their office. Wireless WANs use cellular networks for data transmission. A portable computer with a wireless WAN modem connects to a base station on the wireless networks via radio waves. The radio tower then carries the signal to a mobile switching center, where the data is passed on to the appropriate network. Using the wireless service provider’s connection to the Internet, data communications are established to an organization’s existing network. Wireless WANs use existing cellular telephone networks, so there is also the option of making voice calls over a wireless WAN. Both cellular telephones and wireless WAN PC Cards have the ability to make voice calls as well as pass data traffic on wireless WAN networks.